

Europäisches Patentamt
Europ an Pat nt Offic
Office uropéen d s brev ts



(11) **EP 1 164 555 A2**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
19.12.2001 Bulletin 2001/51

(51) Int Cl.7: **G08B 13/14**

(21) Application number: **01304925.9**

(22) Date of filing: **05.06.2001**

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR**
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **Jespersen, Hans Jacob**
2300 Copenhagen S (DK)

(74) Representative: **Hibbert, Juliet Jane Grace et al**
**Nokia IPR Department Nokia House, Summit
Avenue, Southwood
Farnborough, Hampshire GU14 0NG (GB)**

(30) Priority: **16.06.2000 GB 0014850**

(71) Applicant: **NOKIA MOBILE PHONES LTD.**
02150 Espoo (FI)

(54) **Electronic apparatus including a device for preventing loss or theft**

(57) A mobile telephone includes a control device, which comprises a receiver to receive an enabling signal and a controller to enable operation of the mobile telephone in dependence upon the enabling signal. An active badge transmits the enabling signal. If the telephone and the badge are separated and the mobile telephone is no longer able to receive the enabling signal, then the controller disables the mobile telephone.

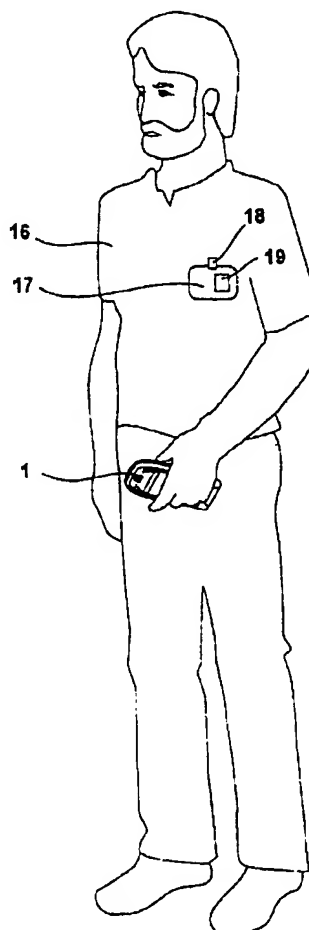


Figure 3

EP 1 164 555 A2

Description

[0001] The present invention relates to a communication unit including a device for preventing loss or theft, in particular, but not exclusive to, mobile telephone handsets and portable computers.

[0002] Portable electronic apparatus are prone to being lost or stolen. Mobile telephone handsets and palm-top computers are particularly vulnerable on account of their compact size and light weight.

[0003] The present invention seeks to help prevent loss or theft of such apparatus.

According to the present invention there is provided electronic apparatus including a device for preventing loss or theft, the device configured to receive and assess an enabling signal from an external source and to control operation of the electronic apparatus in dependence upon said assessment.

[0004] The electronic apparatus may be portable and may be a communications unit, such as a mobile telephone, or a data processing unit, such as a computer. The device may be configured to measure the strength of the enabling signal, to trigger a first alarm if the signal strength is below a first predetermined level and to trigger a second alarm if the signal strength is below a second predetermined level. The enabling signal may include identity information for the external source and the device may be configured to examine said identity information. The device may be configured to trigger an alarm in dependence upon said identity information or to disable operation of the electronic apparatus. The device may be configured to receive a personal identification number and to enable or maintain operation of the electronic apparatus if the personal identification number is received. The device may be configured to receive the enabling signal within a defined timeslot. The device may be configured to perform a first test on information relating to the enabling signal and to report the result of said first test, which may comprise an audible, visual or vibrational alarm. The device may be configured to perform a second test on information relating to the enabling signal and to report the result of said second test, which may also comprise an audible alarm. The electronic apparatus may be configured to be disabled in response to said second test and may be configured to receive a personal identification number in response to said second test. The electronic apparatus may be configured to perform a test on said personal identification number and to enable operation of itself in dependence upon the result of said test on said personal identification number. The device may be configured to receive a personal identification number in response to said second test and to perform a test on said personal identification number. The device may be configured to enable operation of the electronic apparatus in dependence upon the result of said test on said personal identification number.

[0005] The operation of said electronic apparatus

may include operation of all functions of said electronic apparatus. The device may be configured to maintain operation of the apparatus.

[0006] According to the present invention there is also provided a control device for preventing loss or theft, the device configured to receive and assess an enabling signal from an external source and to control operation of the electronic apparatus in dependence upon said assessment.

[0007] According to the present invention there is also provided electronic apparatus incorporating said control device.

[0008] According to the present invention there is also provided control apparatus for preventing loss or theft comprising a first control device configured to transmit an enabling signal and a second control device configured to receive and assess the enabling signal and to control operation of the electronic apparatus in dependence upon the proximity of the first control device.

[0009] The first device may comprise a radio frequency tag or a Bluetooth chip and may be incorporated in a smart card, within a badge, in an item of jewellery, in an article of clothing or in an item of personal property.

[0010] The second control device may be configured to maintain operation of the electronic apparatus.

[0011] According to the present invention there is also provided a system for preventing loss or theft of electronic apparatus, the system comprising electronic apparatus, a first control device configured to transmit an enabling signal and a second control device configured to receive and assess the enabling signal and to control operation of the electronic apparatus in dependence upon said assessment.

[0012] According to the present invention there is also provided a method of preventing loss or theft, the method comprising transmitting an enabling signal and receiving and assessing the enabling signal and controlling operation of the electronic apparatus in dependence upon the assessment.

[0013] According to the present invention there is also provided a method of preventing loss or theft, the method comprising receiving and assessing an enabling signal and to control operation of the electronic apparatus in dependence upon said assessment.

[0014] According to the present invention there is also provided a computer program to be loaded on data processing apparatus to control operation of electronic apparatus so as to prevent loss or theft, such that the data processing apparatus receives information relating to an enabling signal received from an external source, assesses said information and controls operation of the electronic apparatus in dependence upon said assessment.

[0015] The invention will be explained more fully below, by way of example, in connection with preferred embodiments and with reference to the drawings in which:

Figure 1 is a perspective view of a mobile tele-

phon hands t;

Figure 2 is a schematic block diagram of the mobile telephone circuits according to the first embodiment of the present invention;

Figure 3 shows a mobile telephone user wearing a radio frequency (RF) tag according to the first embodiment of the present invention;

Figure 4 is a schematic block diagram of the RF tag according to the first embodiment of the present invention;

Figures 5a, 5b and 5c are parts of a process flow diagram of the interaction between the mobile telephone handset and the RF tag according to the first embodiment of the present invention;

Figure 6 is a schematic block diagram of the mobile telephone circuits according to a second embodiment of the present invention;

Figure 7 is a schematic block diagram of an active badge according to the second embodiment of the present invention;

Figure 8 is a schematic diagram of the functional parts of a Bluetooth chip;

Figure 9 is a sequence diagram showing the transfer of messages between two Bluetooth chips when establishing a wireless connection;

Figure 10 is a process flow diagram of an interaction between the mobile telephone and the active badge according to the second embodiment of the present invention;

Figure 11 is a process flow diagram of the operation of the mobile telephone when a high priority alarm is raised according to either the first or second embodiments;

Figure 12 shows a watch comprising a Bluetooth unit and

Figure 13 is a process flow diagram of an interaction between the mobile telephone and a watch according to the third embodiment of the present invention.

[0016] Referring to Figures 1 and 2, a mobile telephone 1 comprises a case 2, a battery 3, a liquid crystal display (LCD) panel 4, microphone 5, ear-piece 6, keypad 7, antenna 8, subscriber identification module (SIM) card 9, SIM card reader 10 and a ringer 11. The mobile telephone circuitry includes radio interface circuitry 12, codec circuitry 13, controller 14 and memory 15. Indi-

vidual circuits and elements are of a type well known in the art, for example in the Nokia range of mobile telephones.

[0017] Referring to Figures 3 and 4, a user 16 of the mobile telephone 1, wears a contactless proximity smart card badge 17 secured by a clip 18. The badge 17 comprises a radio frequency (RF) identification tag 19 of a type well known in the art. The RF tag 19 comprises a tag antenna 20, a tag transceiver 21, a tag controller 22 and tag memory 23 and is implemented on a semiconductor chip. An example of a suitable RF tag 19 is a tag manufactured according to the Mifare® Architecture Platform produced by Phillips Semiconductors with reference to International Standards Organisation (ISO) 14443A standard, parts 2 and 3.

[0018] The mobile telephone 1 and the RF tag 19 are configured to control operation of the mobile telephone 1 by the transmission and receipt of an enabling signal. The amplitude of a transmitted signal diminishes with distance. Thus, as the separation of mobile telephone 1 and the RF tag 19 increases, if the RF tag 19 transmits a signal, the received signal at the mobile telephone 1 will become weaker and *vice versa*. The rate of signal fall-off with distance can be rapid and significant over a distance of a few meters.

[0019] If the user 16 inadvertently forgets the mobile telephone 1 and walks away from it or a thief steals the telephone 1 and attempts to make away with it, the separation of telephone 1 and the tag 19 increases. As a result, the strength of the signal transmitted by a RF tag 19 and received by the mobile telephone 1 will fade. If the received signal strength falls below a certain threshold or if exchange of signals breaks down, the mobile telephone 1 raises an alarm and, if necessary, disables itself.

[0020] The exchange of signals between the mobile telephone 1 and the RF tag 19 will now be described in more detail.

[0021] Referring to Figures 5a and 5b, the mobile telephone 1 transmits an interrogation signal (step S1), starts a timer (step S2) and begins listening for a reply (step S3). The signal comprises a 64-bit number RAND, randomly generated by the controller 14. In this example, the interrogation signal is transmitted at a frequency in the range of 1 to 2 GHz by the radio interface circuits 12, which are used for communication. It will be appreciated that a separate transceiver may be used instead. It will also be appreciated that other frequencies may be used, for example those specified in ISO 14443A, parts 2 and 3.

[0022] In this example, the RF tag 19 has no power source of its own. It receives power from rectification of the signal from the mobile telephone 1. Thus, the RF tag 19 is inactive until it receives a signal at a particular frequency (step S4) and if the signal is sufficiently strong then RF tag 19 is supplied with power (step S5). It will be appreciated that RF tags may be used that have their own power source, such as a battery or solar cell.

[0023] Once, the RF tag 19 is powered, the tag controller 22 retrieves from tag memory 23 the RF tag's identity label ID_LABEL (step S6). In this example, the RF tag's identity label ID_LABEL is a 64-bit number. The random number RAND is exclusively-ORed with the identity label ID_LABEL to generate an enable code ENABLE (step S7), which is transmitted by the transceiver 21 (step S8). Once the enable signal is transmitted, the power supplied by rectification of the interrogation signal is spent and the RF tag 19 becomes inactive until another signal is received.

[0024] Meanwhile, the mobile telephone 1 waits to receive a reply to its interrogation signal (step S9). If the telephone 1 receives a signal within a predetermined time, for example 100ms, the radio interface circuit 12 measures the power of the signal P (step S10). However, if no signal is received and the counter times out (step S11), the radio interface circuit 12 sets the measured signal power P to zero (step S12).

[0025] Referring to Figure 5c, the mobile telephone 1 assesses the strength and quality of the enable signal. The radio interface circuit 12 determines whether the power of the received signal P is above or below a first non-zero, power level P_1 (step S13). If the received signal power P is below the first power level P_1 , then the controller 14 activates a first level alarm (step S14). In this example, the first level alarm is an audible alarm emitted by the ringer 11. It will be appreciated that other alarms may be used such as a flashing display, illuminated keys and vibration. The radio interface circuit 12 tests whether the power of the received signal P is above or below a second, smaller, non-zero power level P_2 (step S15). If the received signal power P is less than the second power level, the controller 14 activates a second level alarm (step S16). In this example, the second level alarm is also an audible alarm emitted by the ringer 11, but it is louder and higher in pitch than the first alarm. However, other types of alarm may be used. After the second alarm is alerted, the mobile telephone 1 disables itself. It can be re-enabled, for example, by entering a personal identification number (PIN). The second level alarm is explained in more detail later.

[0026] Thus, the first level alarm serves as a gentle reminder to the user 16 to keep the mobile telephone 1 by them, while the second level alarm alerts the user 16 to impending loss or theft of the telephone 1. Furthermore, the second level alarm may also trigger the mobile telephone 1 to activate security features.

[0027] If the received signal power P is above the first power level P_1 or the second power level P_2 , then the controller 14 may optionally examine the enable code ENABLE (steps S17 & S18). This may be used to prevent other RF tags from innocently enabling the mobile telephone 1 or to frustrate attempts to steal the telephone 1 using another RF tag without the alarm sounding.

[0028] The controller 14 retrieves from memory 15 a copy of the RF tag's identity label ID_LABEL and exclu-

sively-ORs the label with the randomly generated number RAND to generate a local version of the enable code LOCAL. The controller 14 compares the local enable code LOCAL with the received enable code ENABLE. If they match, the received enable code ENABLE is verified as being authentic and the mobile telephone 1 continues to operate. The process repeats itself by generating and transmitting a new random number RAND (step S1). The process may be repeated, for example every 10 seconds. If the local enable code LOCAL and the received enable code ENABLE do not match, the received enable code ENABLE is rejected as being a forgery and the mobile telephone 1 activates the second level alarm (step S16).

[0029] It will be appreciated that the random number RAND and the enable code ENABLE may be encrypted before transmission. It will also be appreciated that the mobile telephone 1 may be configured to check the result of the comparison, for example by repeating the process with a new random number, to allow for innocent corruption of the code or collision of several enable codes transmitted by different RF tags. Alternatively, the mobile telephone 1 may be configured to allow receipt of several enable codes and search through them until the correct enable code is found.

[0030] Thus, while the mobile telephone 1 and the RF tag 19 are close enough together, the RF tag 19 will receive a strong enough signal to operate and process the interrogation signal and return an enabling signal to the mobile telephone 1 to allow the mobile telephone 1 to operate.

[0031] The first embodiment describes a badge, which transmits an enabling signal in response to a prompt from the mobile telephone 1. The second embodiment is a modification, which, amongst other things, allows the badge to send an enable unprompted.

[0032] Referring to Figures 1 and 6, the mobile telephone 1 shown in Figures 1 and 2 is modified to include a first Bluetooth™ chip 24.

[0033] Referring to Figure 7, the badge 17 shown in Figure 3 is replaced by an active badge 25 with a clip 26 comprising a second Bluetooth™ chip 27 powered by a battery 28.

[0034] Referring to Figure 8, the first and second Bluetooth™ chips 24, 27 comprise a transceiver 29, a link controller 30 to control the physical establishment of the radio link and a link manager 31 to manage the execution of link protocols and to interface with an electronic device. In this example, the first Bluetooth chip 24 is interfaced with the mobile telephone controller 14.

[0035] The Bluetooth™ system allows electronic devices to communicate with each other using short-range radio links. The system is configured to connect between two and eight devices to form a "piconet". One device in the piconet serves as the master unit and its clock is used to synchronise communication throughout the piconet. Both voice and data may be communicated through the piconet. Overlapping piconets may be

linked together to form a "scattered network". A Bluetooth™ specification (version 1.0 B) and a system overview may be found on the world-wide web at www.bluetooth.com or ordered from Bluetooth SIG, c/o Daniel Edlund, Facsimile No.: +46 70 615 9049.

[0036] Referring to Figure 9, a brief overview of how a connection is established between the first and second Bluetooth™ chips 24, 27 will now be described. Under normal conditions, the first chip 24 operates in a low-power consumption standby mode. The first chip 24 periodically "wakes-up" and enters an inquiry mode and repeatedly broadcasts inquiry message over a set of frequencies, inviting other devices to respond (step S19). The inquiry message may specify that only certain types of devices should respond and this is specified as an access code at the beginning of the message. Having broadcast an inquiry message, the first chip 24 listens for inquiry response messages on a different set of frequencies. The second chip 27 receives the inquiry message and replies with an inquiry response message, which contains its device address (step S20).

[0037] The first chip 24, now in possession of the second chip's device address, passes into page mode. A page message is transmitted using a hopping sequence determined by the device address (step S21). The second chip 27 receives the page message and replies by sending a page response message (step S22). The process by which the second chip 27 begins to synchronise to the first unit's clock now begins. The first chip 24 sends a special control packet that includes information relating to its clock data and the channel hopping sequence to be used and a second chip 27 confirms receipt with a response (steps S23 & S24). The first and second chips 24, 27 are now in a connected state and can begin exchanging packets of data (step S25) and are connected by means of a piconet. Higher level protocols manage the exchange of information between the mobile telephone 1 and the badge 25.

[0038] The second chip 27 in the connected state can operate in several modes. In an active mode, the second chip 27 listens to time and frequency slots for data packets from the first chip 24 and then sends data packets in other allocated slots. However, if no data is being transferred then the first chip 24 can arrange for the second chip 27 to be put in a power-saving mode. In such a mode, a hold mode, an internal timer is started and the second chip 27 becomes inactive for a fixed duration. Alternatively, the second chip 27 may be placed into sniff mode during which it polls the piconet at a reduced rate. Finally, the second chip 27 may be placed in park mode, wherein it surrenders its device address and does not participate in data traffic.

[0039] The radio transceivers operate at a 2.4 GHz and have a broadcast range of up to 100m. The amplitude of a transmitted signal diminishes with distance. Thus, as the separation of mobile telephone 1 and the active badge 25 increases, if the active badge 25 transmits a signal, the received signal at the mobile telephone

1 will become weaker and *vice versa*. The rate of signal fall-off with distance can be rapid and significant over a distance of a few meters.

[0040] If the user 16 inadvertently forgets the mobile telephone 1 and walks away from it or a thief steals the telephone 1 and attempts to make away with it, the separation of telephone 1 and the badge 25 increases. As a result, the strength of the signal transmitted by the active badge 25 and received by the mobile telephone 1 will fade. If the received signal strength falls below a certain threshold or if the piconet breaks down, the mobile telephone 1 is configured to raise an alarm and, if necessary, disable itself.

[0041] Referring to Figures 9 and 10, the second chip 27, located in the badge 25, periodically sends a message to the first chip 24 in an allocated time slot (step not shown). The message contains the second chip's address by which it may be identified. The first chip 24 checks to see if it receives a message in the time slot (steps S26 & S27). If the first chip 24 receives the message in the correct timeslot, it proceeds to measure the power of the signal S (step S28), otherwise it sets the measured power of the signal S to zero (step S29).

[0042] The first chip 24 determines whether the power S of the received signal is below the first power level S_1 (step S30). If the received signal power S is below the first power level S_1 , then the first chip 24 alerts the mobile telephone controller 14, which activates a first level alarm, for example an audible alarm emitted by the ringer 11 (step S31). Other types of alarms as described hereinbefore may be used.

[0043] The first chip 24 tests whether the power of the received signal S is below a second, lesser, non-zero power level S_2 (step S32). If the received signal power S is less than the second power level S_2 , the first chip 24 notifies the mobile telephone controller 14, which activates a second level alarm (step S33). In this example, the second level alarm is an audible alarm emitter by the ringer 11, louder and higher in pitch than the first alarm. Furthermore, the mobile telephone 1 is disabled and requires entering of a personal identification number (PIN) before it can be used again.

[0044] If the received signal power S is above the first power level S_1 or the second power level S_2 , then the chip 24 checks the address of the message (steps S34 & S35). If the address is that of the second chip 27, the mobile telephone 1 continues operation, otherwise it alerts the mobile telephone controller 14 (step S33).

[0045] Thus, while the mobile telephone 1 and the active badge 25 are close enough together, the two Bluetooth chips 24, 27 form a piconet. If the piconet breaks down or the signals become too weak, then the mobile telephone 1 raises an alarm.

[0046] It will be appreciated that the Bluetooth chips may communicate in different ways to that described above. The enabling signal may be triggered in response to an enquiry by the Bluetooth™ chip 24 in the mobile telephone 1. Furthermore, the mobile telephone 1

may process the enabling signal in a different manner. Alternatively, the piconet may be used to exchange a plurality of messages, the receipt of which is necessary to allow the mobile telephone to continue operation.

[0047] The mobile telephone 1 is provided with security features to prevent unauthorised use. For example, whenever the mobile telephone 1 is switched on, the user 16 is asked to enter a four-digit PIN on the keypad 8. If the correct PIN is entered, the mobile telephone 1 continues to operate. If an incorrect number is entered then the user is permitted another attempt. If the correct PIN number is not entered by the third attempt then use of the mobile telephone 1 is barred. The mobile telephone 1 switches itself off.

[0048] Referring to Figures 5c, 10 and 11, if the second level alarm is raised (steps S16 or S33), then the mobile telephone 1 sounds a loud, high-pitched alarm on the ringer 11 (step S16.1, step S33.1). The LCD panel 5 displays a request to enter a PIN (step S16.2, step S33.2). The mobile telephone 1 waits until a 4-digit number is entered on the keypad 7 (step S16.3, step S33.3) and checks whether the number matches the PIN (step S16.4, step S33.4). In this example, the PIN is the same as the user-defined PIN entered on the keypad 7 whenever the mobile telephone 1 is switched on. Alternatively, it may be a different number and may have any number of digits. If the correct PIN is entered then the mobile telephone 1 continues to operate (step S16.5, step S33.5). If an incorrect number is entered, then the operator, who may be the user 16, is allowed another two attempts (step S16.6, step S33.6). If an incorrect number is entered three times, then the mobile telephone 1 is barred from further use and it switches itself off (step S16.7, step S33.7). This prevents unauthorised use.

[0049] The second embodiment comprises a single active badge 25 and a single mobile telephone 1. The third embodiment is a modification of the second embodiment in which the user 16 holds more than one Bluetooth unit, for example one in the form of an active badge 25 and one in an article of jewellery, such as a watch.

[0050] In Figure 12, a watch 32 is shown comprising a third Bluetooth chip 33. When in close proximity, the first, second and third Bluetooth units 24, 27, 33 form a piconet. In this example, the first Bluetooth unit 24 in the mobile telephone 1 is the master unit.

[0051] Referring to Figure 13, the first Bluetooth unit 24 checks whether it has received an enabling signal S from the second Bluetooth unit 27 in a similar manner described hereinbefore (steps S36 & S37). In this example, however, the first chip 24 checks whether the received signal power S is below the second power level S_2 . If the received signal power S falls below the second power level S_2 , then the first chip 24 checks whether it has received a further enabling signal S' from the third Bluetooth unit 33 (steps S38 & S39). If the power of the further signal S' falls below the second power level S_2 , then the first chip 24 alerts the mobile telephone con-

troller 14, which activates the second level alarm and disables the mobile telephone 1 as described hereinbefore (step S40). Thus, the alarm is activated when both the badge 25 and the watch 32 are out of range of the piconet formed with the mobile telephone 1. It will be appreciated that the user 16 can hold more than two Bluetooth units, in a variety of articles, including clothing, jewellery and other personal items, and that they may be selectively activated or deactivated. The piconet allows up to eight Bluetooth units to participate, so allowing the user to hold up to seven Bluetooth units. Furthermore, the mobile telephone 1 may be programmed to trigger one or more alarms according to different received signal power conditions. For example, the process described with reference to Figure 13 may include both first and second level alarms.

[0052] The fourth embodiment is a variation of the third embodiment in which the user 16 holds a Bluetooth unit, for example one in the form of an active badge 25, and more than one piece of equipment such as a mobile telephone 1 and a laptop computer each hold Bluetooth units respectively. Thus, if either the telephone 1 or the computer become separated from the badge 25 then they activate an alarm.

[0053] The first Bluetooth unit 24 checks whether it has received the enabling signal S from the second Bluetooth unit 27 according to the procedure described with reference to Figure 10. In this example, a laptop computer (not shown) having a fourth Bluetooth chip (not shown) also checks whether it has received the enabling signal S and independently executes the same procedure. Thus, if either the telephone 1 or the computer become separated from the badge 25 then they emit an alarm. It will be appreciated that the Bluetooth units may cooperate such that if either the telephone or the computer wanders away and become separated from the badge 25, then both the wandering and the remaining pieces of equipment activate alarms. This may be co-ordinated by the master unit, which may be the second Bluetooth unit 27 located in the badge 25 or article of jewellery.

[0054] It will be appreciated that while the invention has been described in relation to mobile telephones, it can be used with any sort of portable electronic apparatus, for example, hand held computers.

[0055] It will be appreciated that many modifications may be made to the embodiments described above. For example, the RF tag or the Bluetooth chip may be incorporated into a piece of jewellery, such as a ring or medallion or into an item of personal property such as a handbag.

[0056] The apparatus may also be used to prevent unauthorised use of and theft from a cash register. The cash register is fitted with a receiver and a controller or a Bluetooth unit. A till operator keeps on or about them an RF tag or active badge. The cash register may only operate when the till operator is present at the cash register.

Claims

1. A communication unit including a device for preventing loss or theft, the device configured to receive and assess an enabling signal from an external source and to control operation of the electronic apparatus in dependence upon said assessment, said device being configured to measure the strength of the enabling signal and to examine an identity information included in said enabling signal, further being configured to trigger a first alarm if the signal strength is below a first predetermined level **characterised in that** the device is further configured to trigger a second alarm if the signal strength is below a second predetermined level.
2. A communication unit according to claim 1 **characterised in that** the device is configured to disable operation of the communication unit.
3. A communication unit according to claim 1 or 2 **characterised in that** the device is configured to receive a personal identification number.
4. A communication unit according to claim 3 **characterised in that** the device is configured to enable operation of the communication unit if the personal identification number is received.
5. A communication unit according to any one of claims 1 to 4 **characterised in that** it is configured to receive the enabling signal within a defined timeslot.
6. A communication unit according to any preceding claim **characterised in that** the device is configured to perform a first test on information relating to the enabling signal.
7. A communication unit according to claim 6 **characterised in that** the device is configured to perform a second test on information relating to the enabling signal.
8. A communication unit according to claim 7 **characterised in that** the device is configured to report the result of said first and second test.
9. A communication unit according to claim 8 **characterised in that** said report of said first test or said second test comprises an audible alarm.
10. A communication unit according to claim 8 or 9 **characterised in that** said report of said first test or said second test comprises a visual alarm.
11. A communication unit according to any one of claims 7 to 10 **characterised in that** it is configured to be disabled in response to said second test.
12. A communication unit according to any one of claims 7 to 10 **characterised in that** it is configured to receive a personal identification number in response to said second test.
13. A communication unit according to claim 12 **characterised in that** it is configured to perform a test on said personal identification number.
14. A communication unit according to claim 13 **characterised in that** it is configured to enable operation of itself in dependence upon the result of said test on said personal identification number.
15. A communication unit according to any one of claims 7 to 10 **characterised in that** the device is configured to receive a personal identification number in response to said second test.
16. A communication unit according to claim 15 **characterised in that** the device is configured to perform a test on said personal identification number.
17. A communication unit according to claim 16 **characterised in that** the device is configured to enable operation of the communication unit in dependence upon the result of said test on said personal identification number.
18. A communication unit according to any preceding claim **characterised in that** the operation of said communication unit includes operation of all functions of said communication unit.
19. A communication unit according to any preceding claim **characterised in that** it comprises a data processing unit.
20. A communication unit configured for preventing loss or theft, the device configured to receive and assess an enabling signal from an external source and to control operation of the electronic apparatus in dependence upon said assessment **characterised in that** the unit comprises a first control device configured to transmit an enabling signal and a second control device configured to receive and assess the enabling signal and to control operation of the communication unit in dependence upon the proximity of the first control device.
21. A communication unit according to claim 20 **characterised in that** the first device comprises a radio frequency tag.
22. A communication unit according to claim 20 **characterised in that** the first device comprises a Bluetooth chip.

23. A communication unit according to any one of claims 20 to 22 **characterised in that** the first device is incorporated in a smart card.
24. A communication unit according to any one of claims 20 to 22 **characterised in that** the first device is incorporated within a badge. 5
25. A communication unit according to any one of claims 20 to 22 **characterised in that** the first device is incorporated in an item of jewellery. 10
26. A communication unit according to any one of claims 20 to 23 **characterised in that** the first device is incorporated in an article of clothing. 15
27. A communication unit according to any one of claims 20 to 23 **characterised in that** the first device is incorporated in an item of personal property. 20
28. A device according to claim 27 **characterised in that** the communication unit is a mobile telephone.
29. A device according to claim 27 **characterised in that** the communication unit is a computer. 25
30. A system for preventing loss or theft of communication unit, the system comprising:
- a communication unit; 30
 - a first control device configured to transmit an enabling signal and
 - a second control device configured to receive and assess the enabling signal and to control operation of the communication unit in dependence upon said assessment. 35
31. A method of preventing loss or theft, the method comprising: 40
- transmitting an enabling signal and
 - receiving and assessing the enabling signal and
 - controlling operation of the communication unit in dependence upon the assessment. 45
32. A computer program to be loaded on data processing apparatus to control operation of a communication unit so as to prevent loss or theft, such that the data processing apparatus receives information relating to an enabling signal received from an external source, assesses said information and controls operation of the communication unit in dependence upon said assessment. 50
- 55

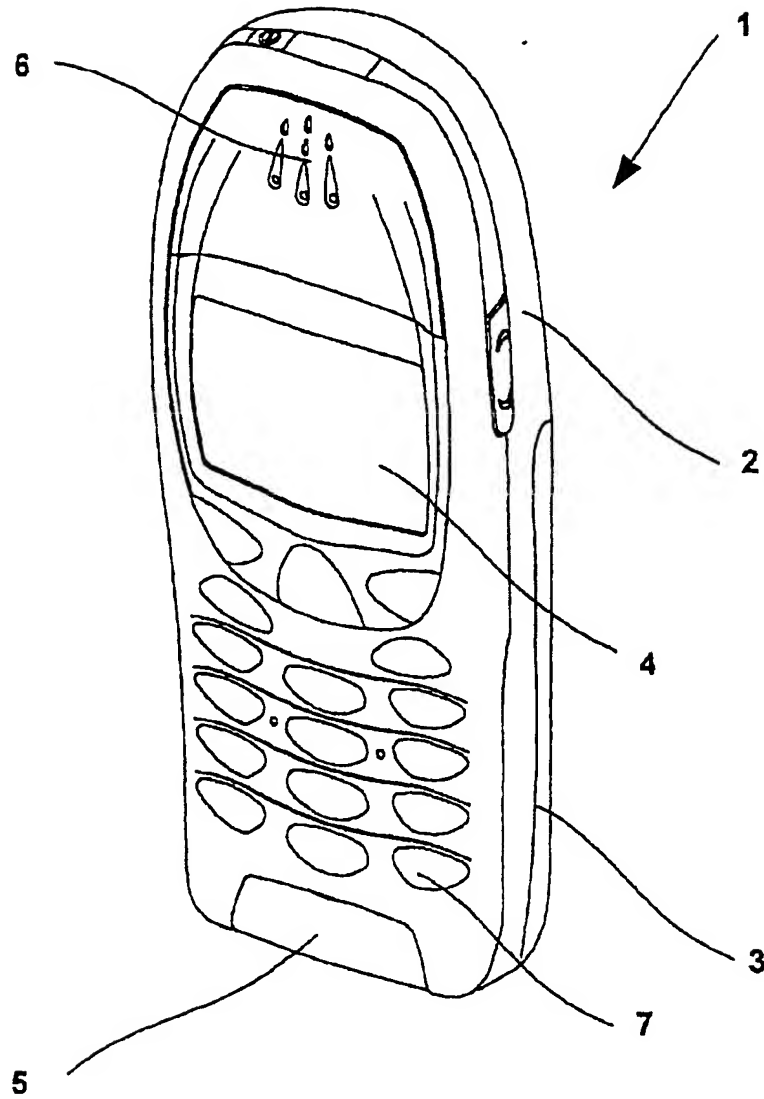


Figure 1

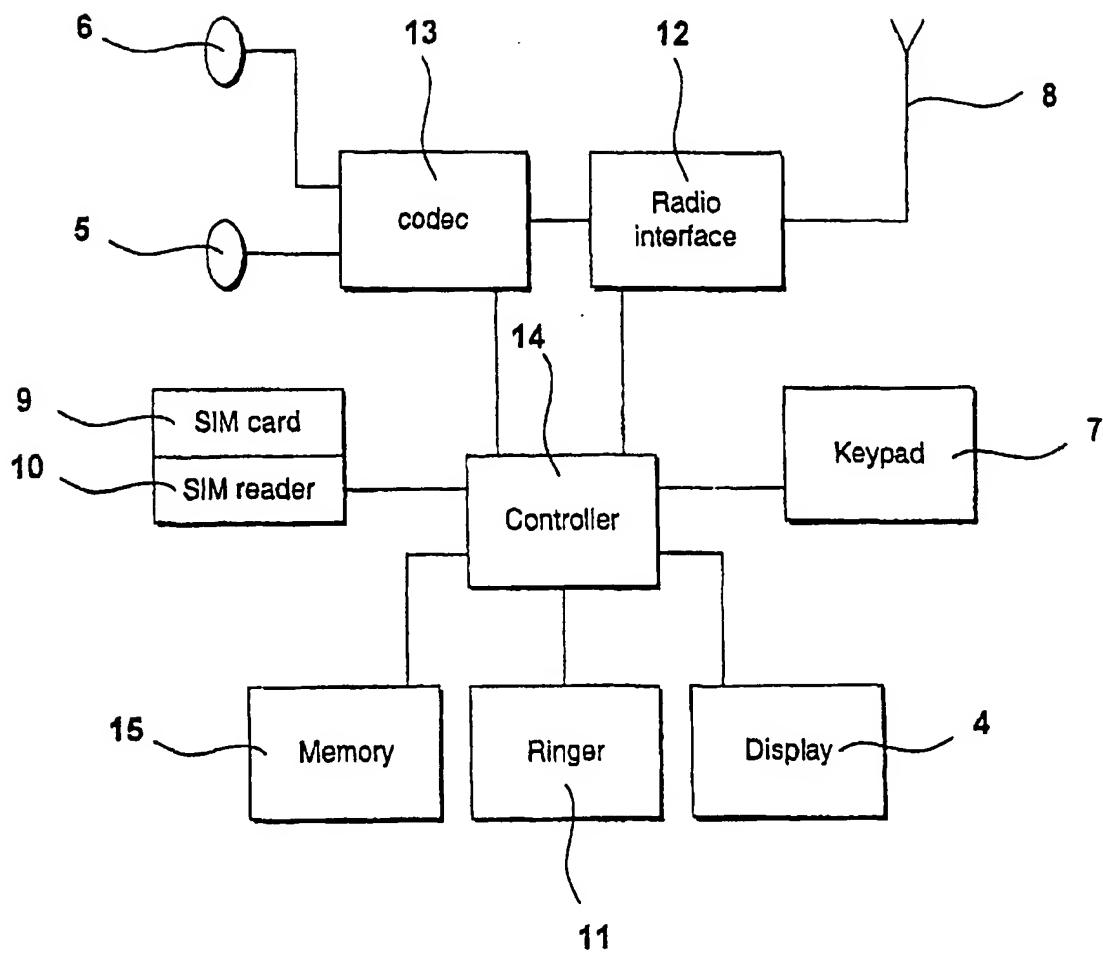


Figure 2

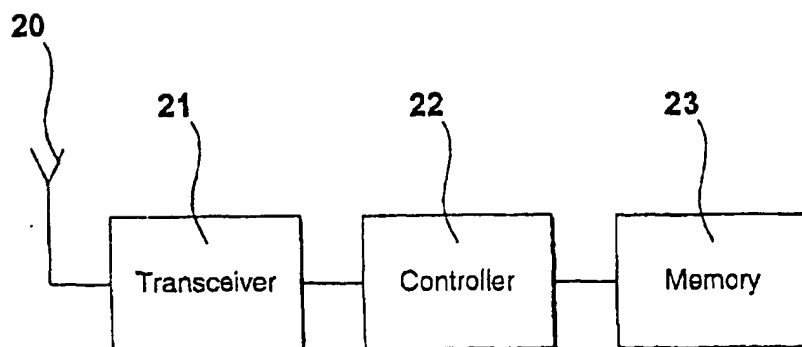


Figure 4

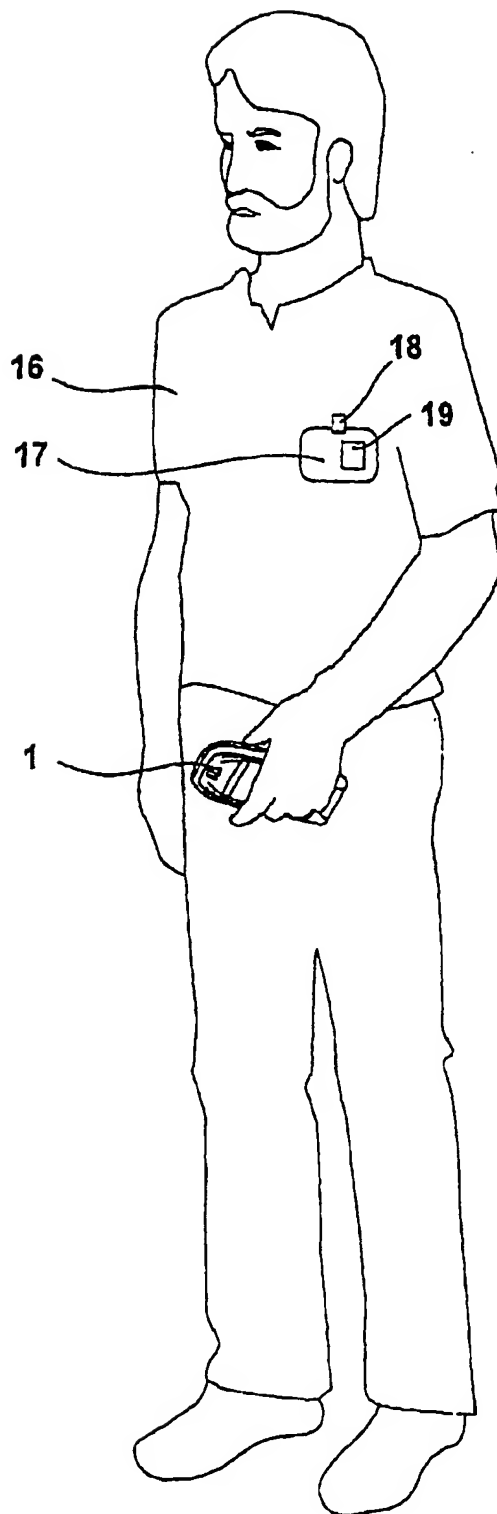


Figure 3

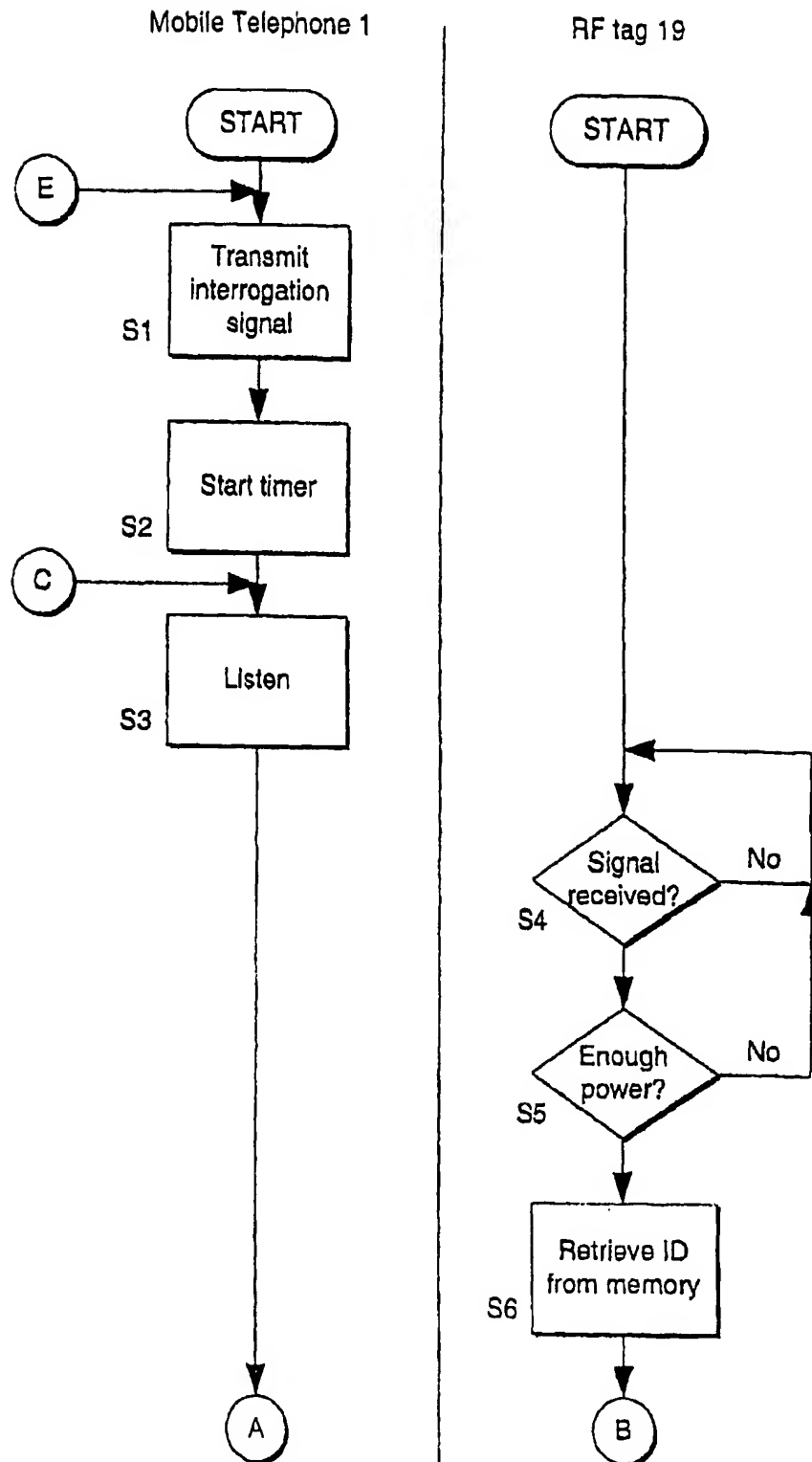


Figure 5a

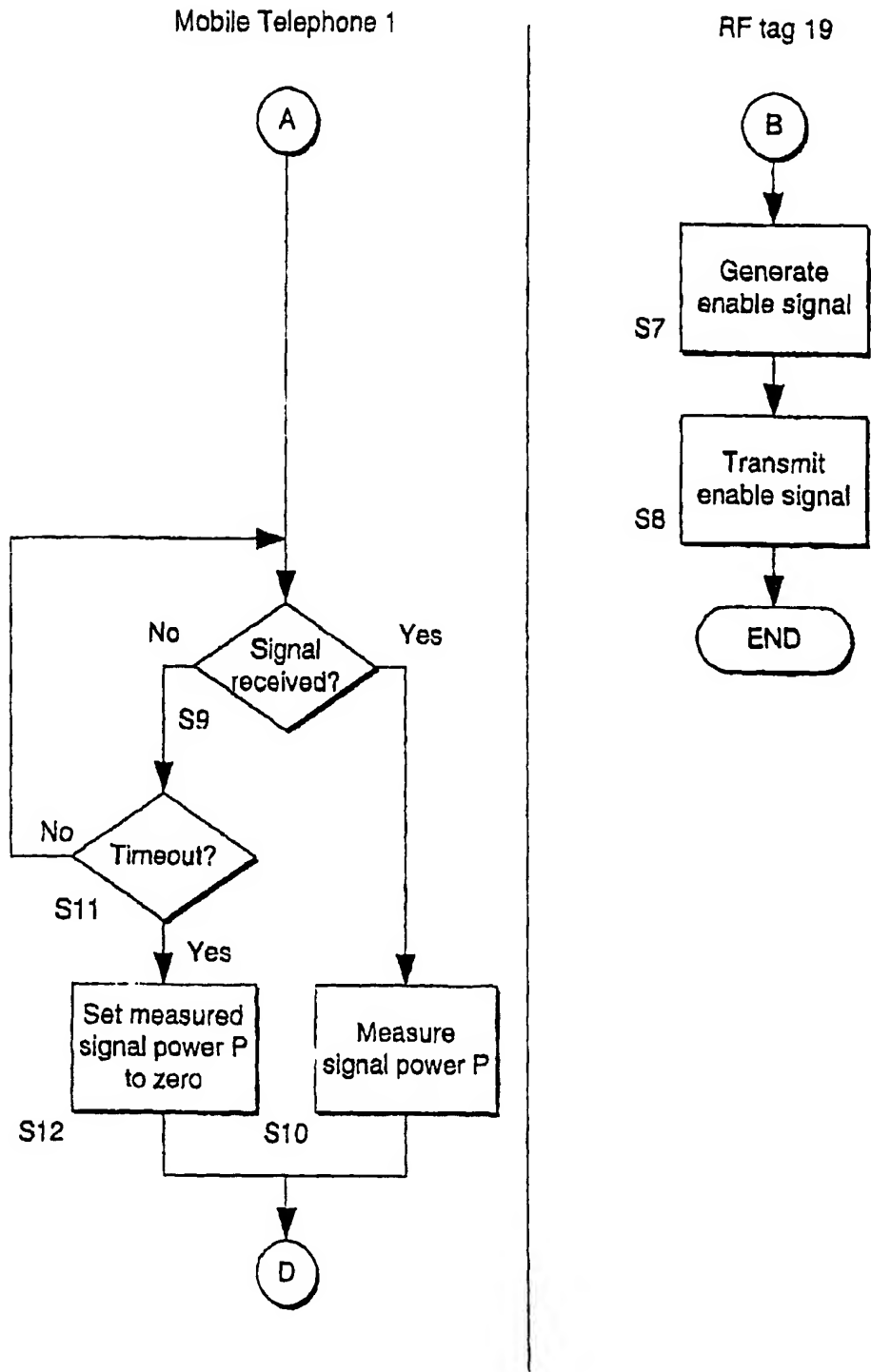


Figure 5b

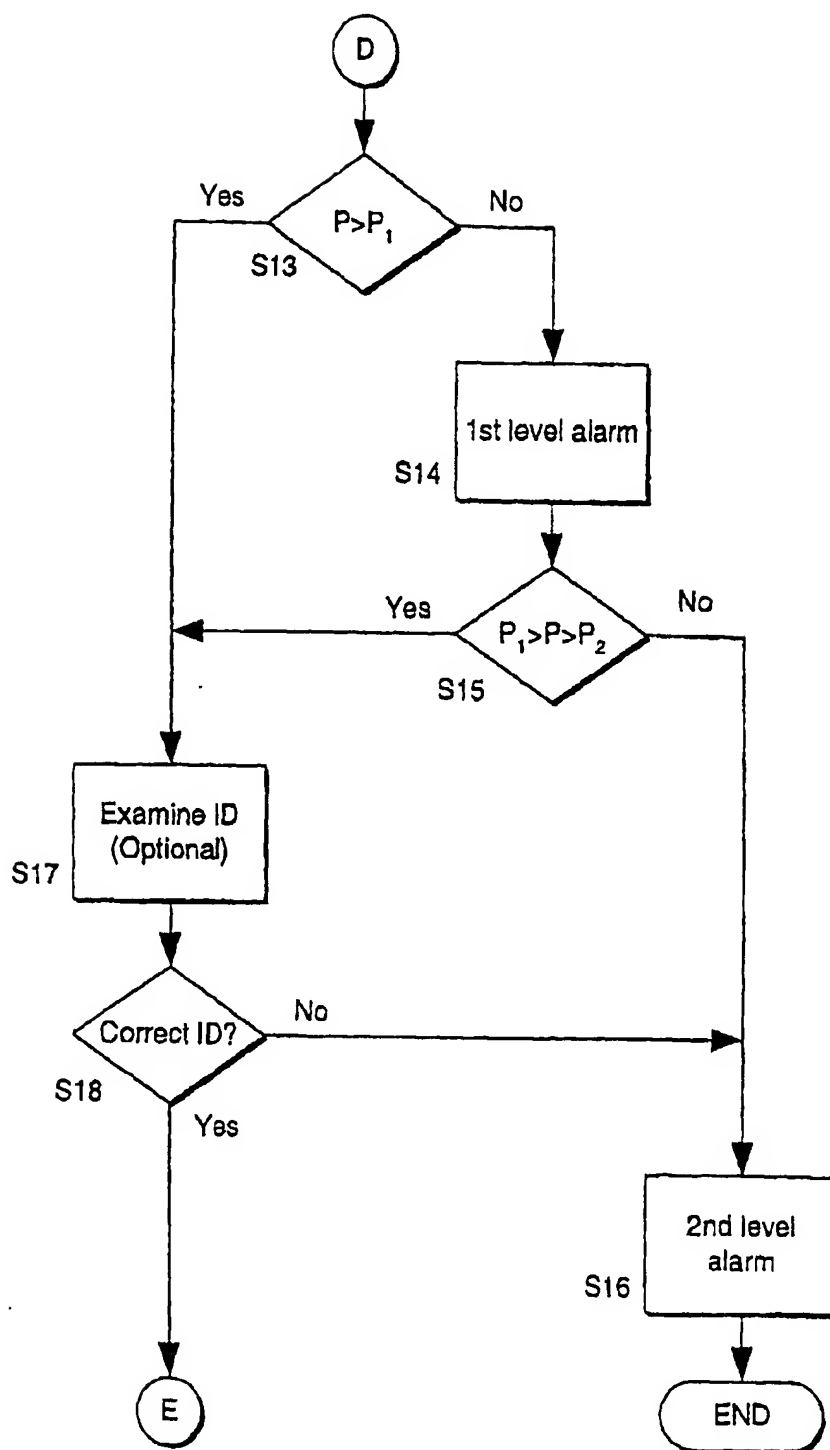


Figure 5c

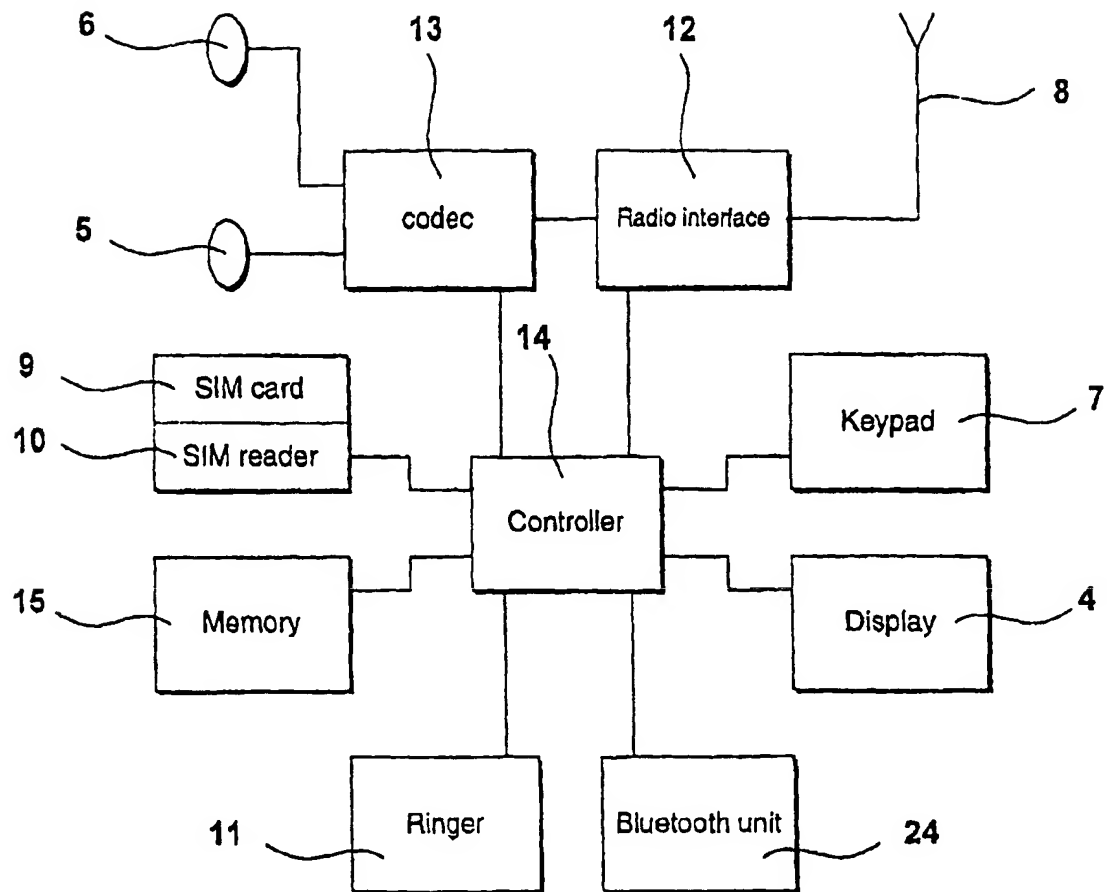


Figure 6

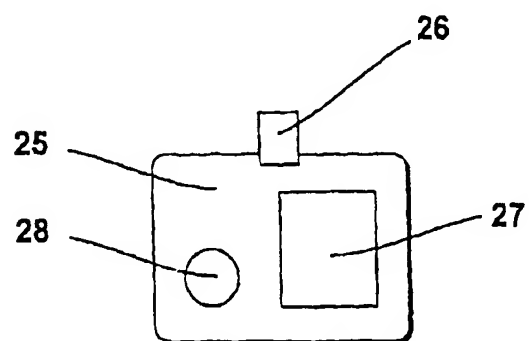


Figure 7

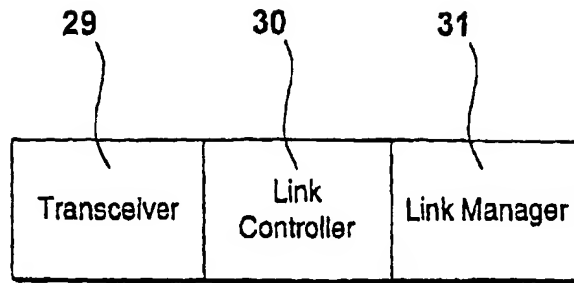


Figure 8

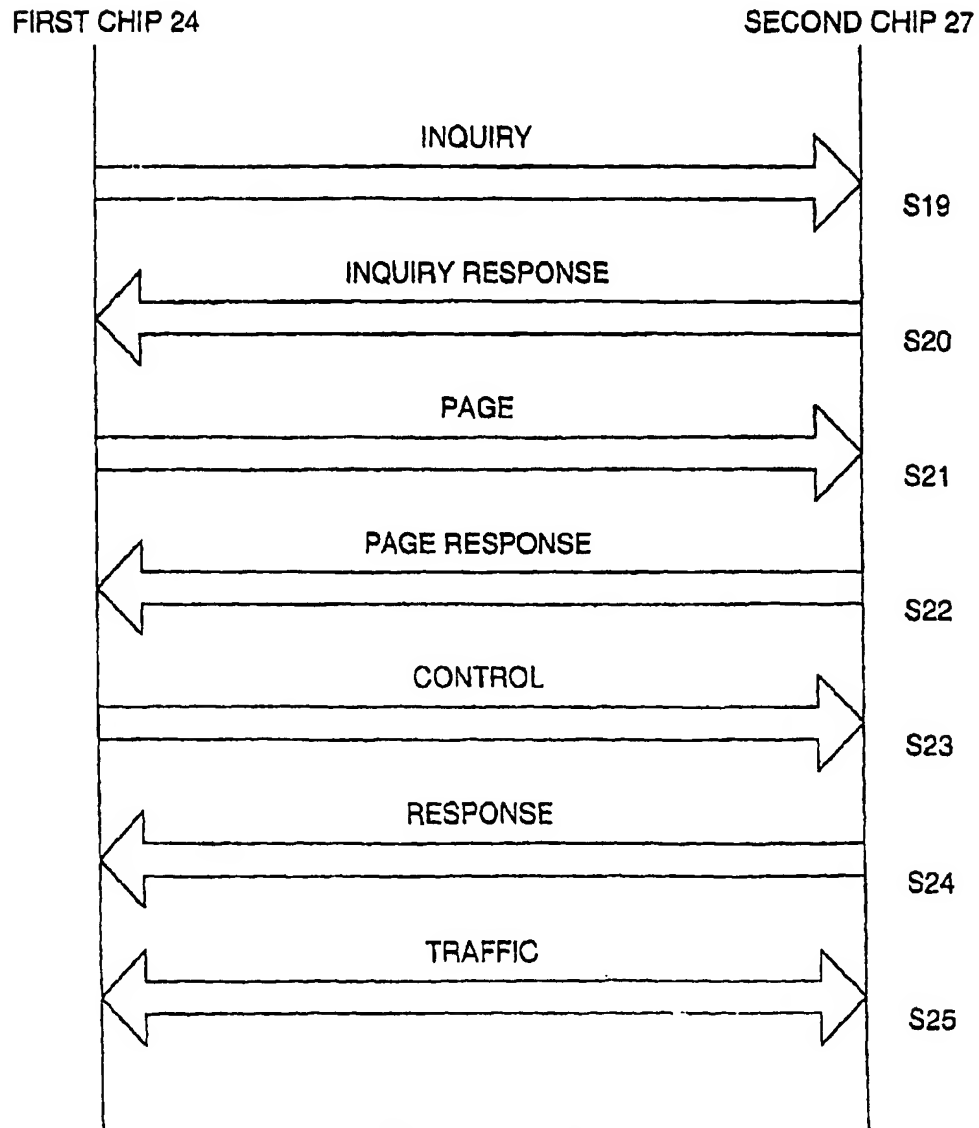
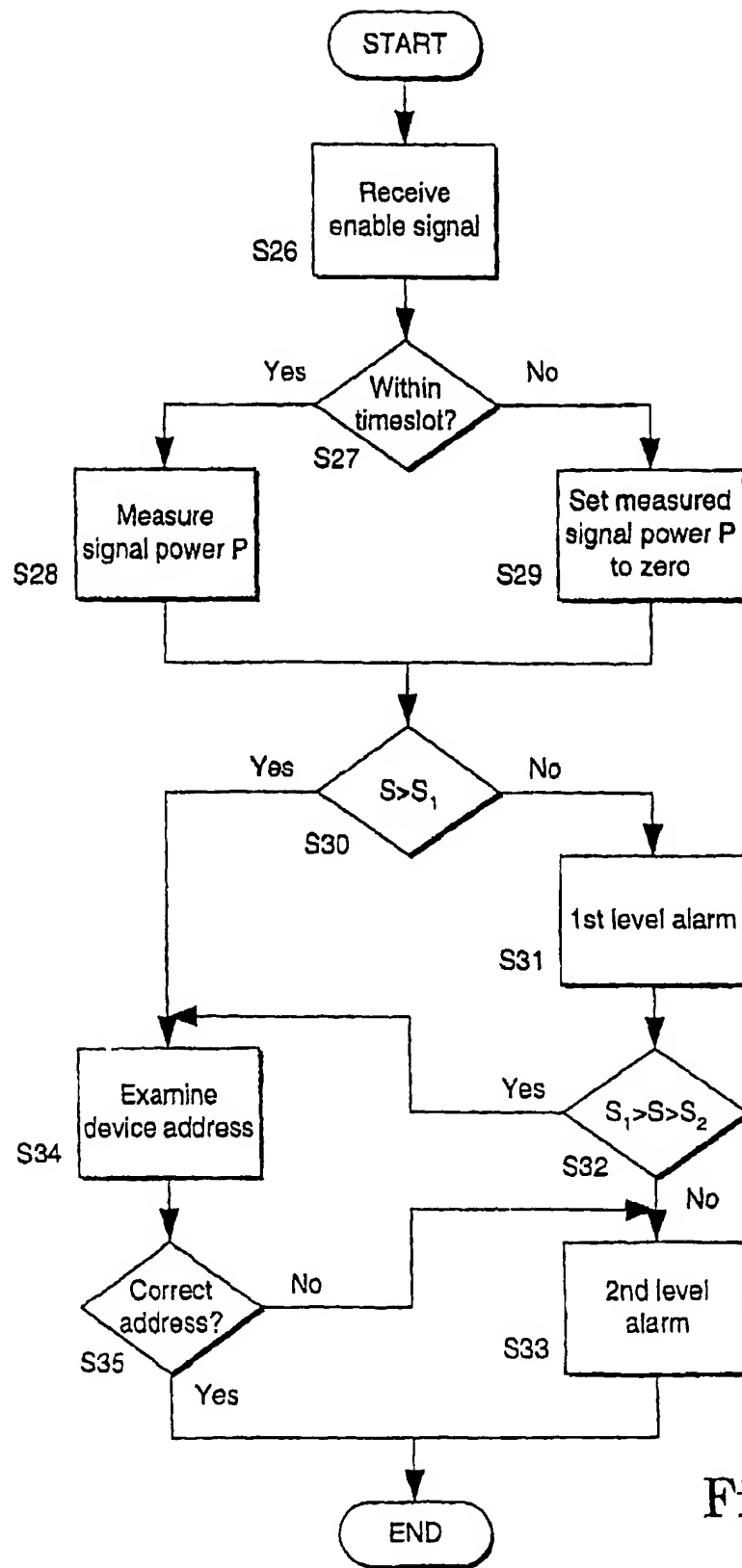


Figure 9

Figure
10

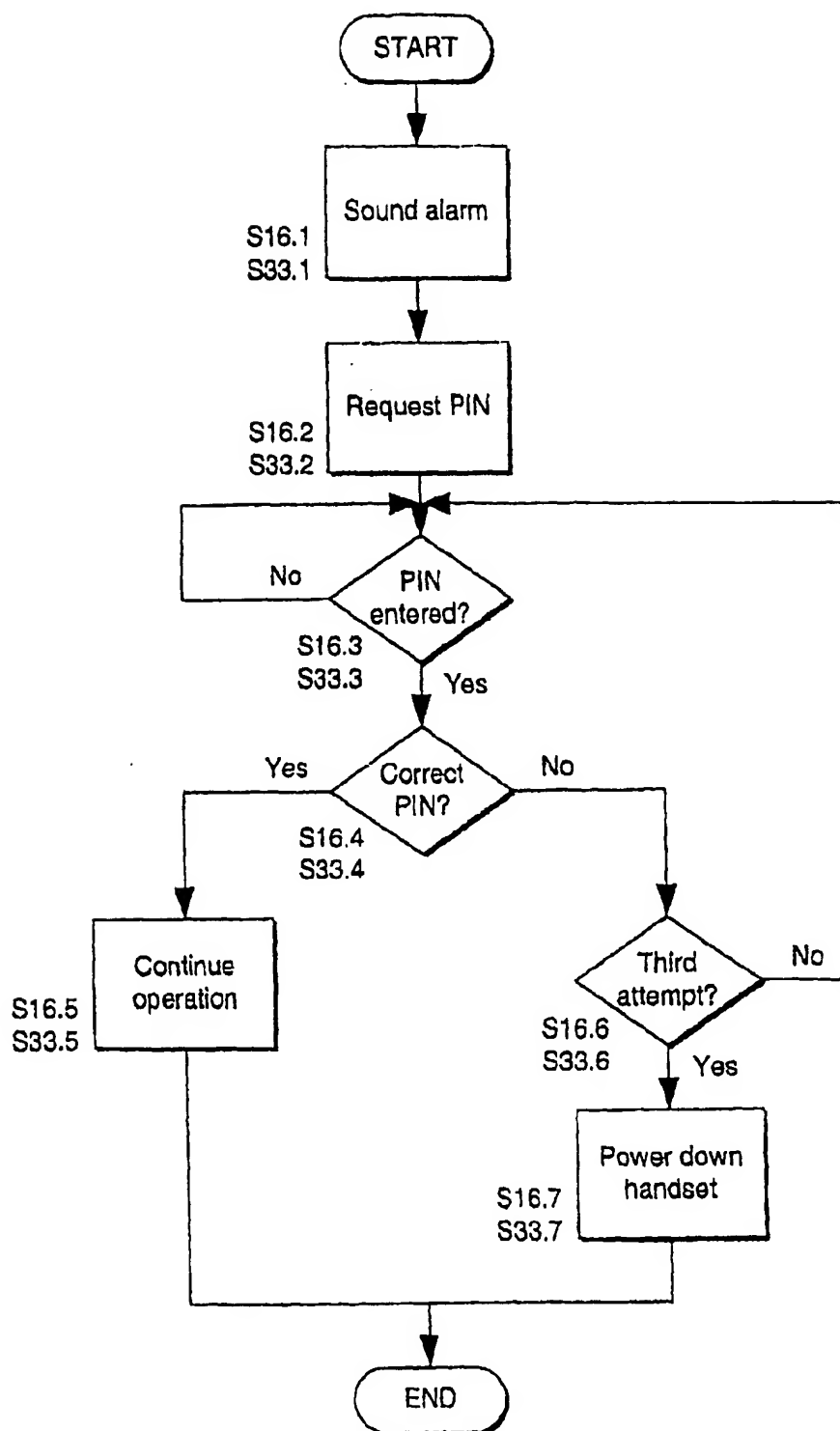


Figure
11

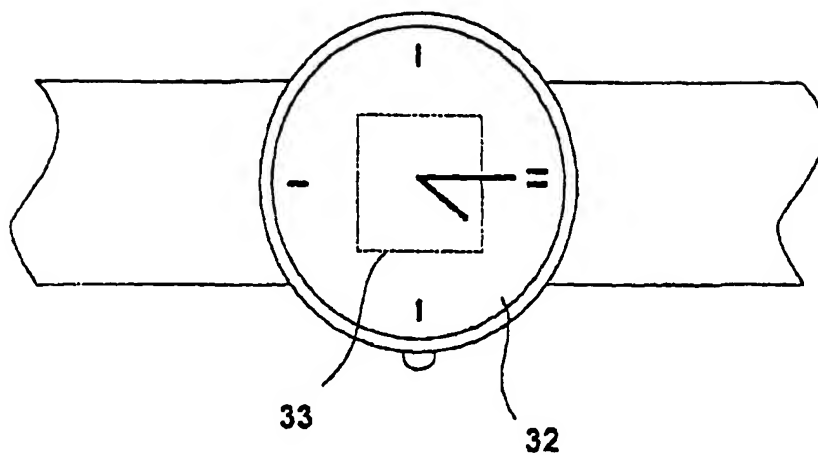


Figure
12

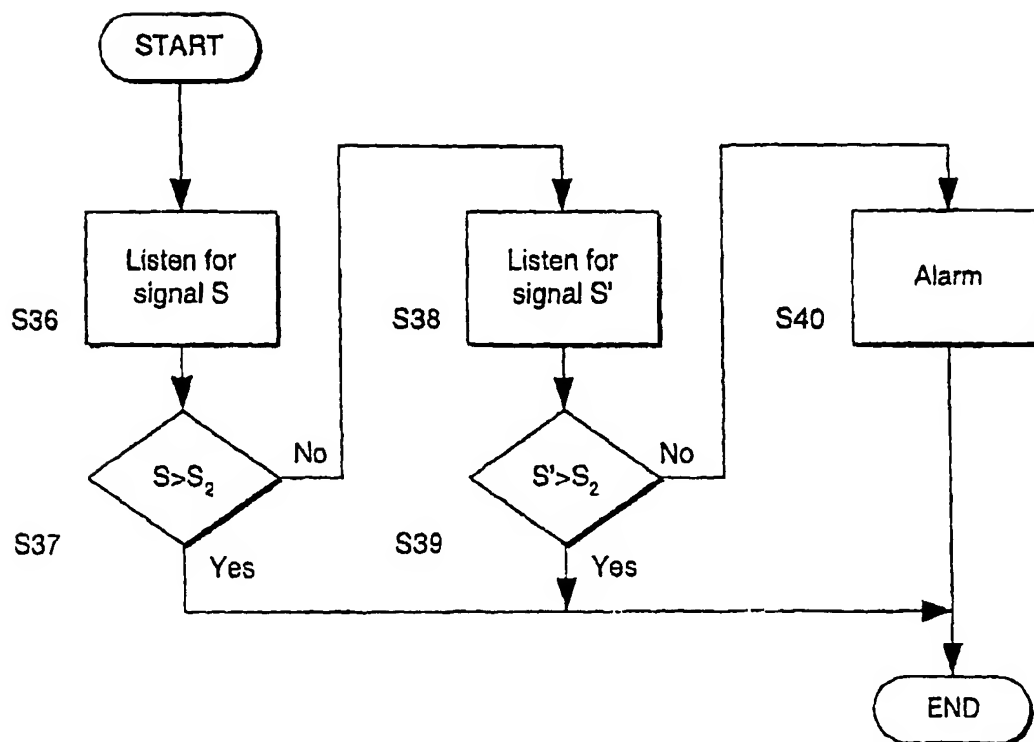


Figure
13



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) **EP 1 164 555 A3**

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
19.06.2002 Bulletin 2002/25

(51) Int Cl.7: **G08B 13/14, G08B 21/24**

(43) Date of publication A2:
19.12.2001 Bulletin 2001/51

(21) Application number: **01304925.9**

(22) Date of filing: **05.06.2001**

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR**
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **Jespersen, Hans Jacob**
2300 Copenhagen S (DK)

(74) Representative: **Hibbert, Juliet Jane Grace et al**
Nokia IPR Department
Nokia House,
Summit Avenue,
Southwood
Farnborough, Hampshire GU14 0NG (GB)

(30) Priority: **16.06.2000 GB 0014850**

(71) Applicant: **Nokia Corporation**
02150 Espoo (FI)

(54) **Electronic apparatus including a device for preventing loss or theft**

(57) A mobile telephone includes a control device, which comprises a receiver to receive an enabling signal and a controller to enable operation of the mobile telephone in dependence upon the enabling signal. An active badge transmits the enabling signal. If the telephone and the badge are separated and the mobile telephone is no longer able to receive the enabling signal, then the controller disables the mobile telephone.

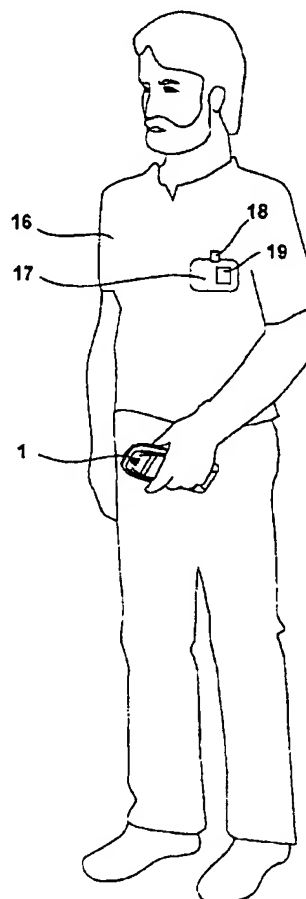


Figure 3

EP 1 164 555 A3



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 30 4925

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	GB 2 318 671 A (NOKIA MOBILE PHONES LTD) 29 April 1998 (1998-04-29)	1-4,20, 27,28, 30-32 5-11,19	G08B13/14 G08B21/24
Y	* figures 8,9 * * page 10, paragraph 3 * * page 11, paragraph 2 * ---		
X	JP 11 088499 A (SASAKURA TOYOKI;MIYAKEN KEIEI SENRIYAKU KENKYUSHO:KK) 30 March 1999 (1999-03-30)	20,23, 27-32	
A		1	
Y	& US 6 151 493 A (SASAKURA TOYOKI ET AL) 21 November 2000 (2000-11-21) * column 2, line 45 - line 65 * * column 3, line 56 - line 58 * * column 4, line 52 - line 61 * * column 5, line 1 - line 15 * * column 9, line 19 - line 23 * ---	5-11,19	
X	US 5 796 338 A (MARDIROSSIAN ARIS) 18 August 1998 (1998-08-18)	30	TECHNICAL FIELDS SEARCHED (Int.Cl.7)
A	* column 2, line 14 - line 42 * -----	1,20	G08B
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 25 April 2002	Examiner De la Cruz Valera, D
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons</p> <p>& : member of the same patent family, corresponding document</p>			

EPO FORM 1503 (01.02.92) (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 01 30 4925

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-04-2002

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
GB 2318671	A	29-04-1998	NONE		

JP 11088499	A	30-03-1999	JP	2931276 B2	09-08-1999
			US	6151493 A	21-11-2000

US 5796338	A	18-08-1998	EP	0962103 A1	08-12-1999
			WO	9834417 A1	06-08-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82